Global Federated Identity and Privilege Management (GFIPM)

John Wandelt

Georgia Tech Research Institute (GTRI)

August 2007

Global Justice Information Sharing Initiative

What's in your wallet?

The Challenge

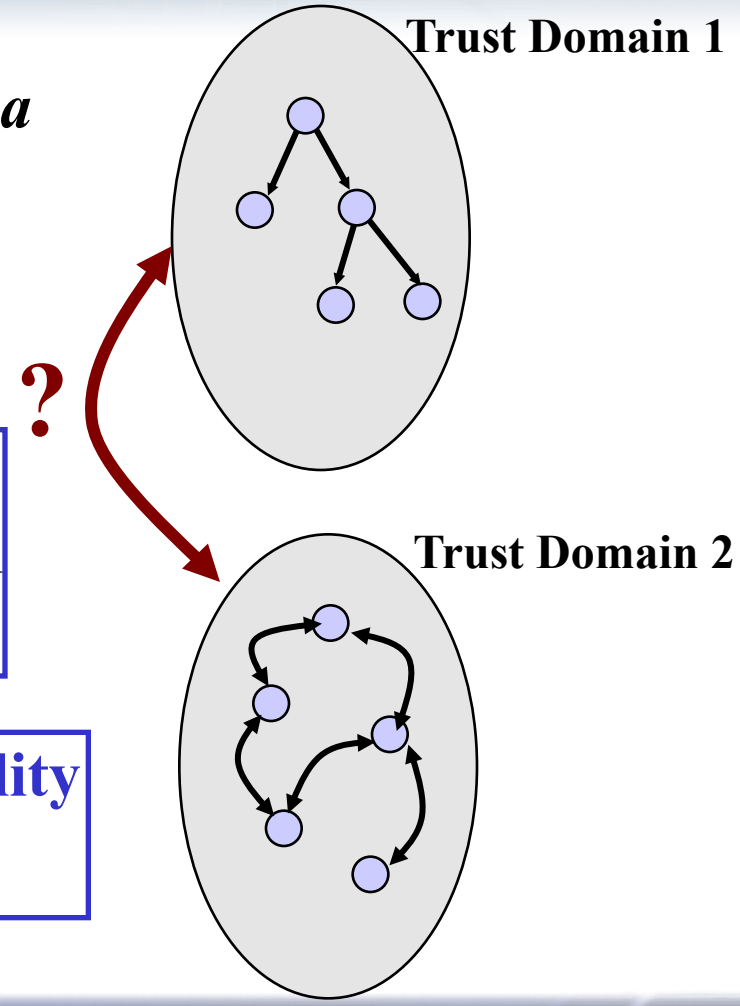
- Many recognized sensitive but unclassified (SBU) networks and information systems
- Each have investments in technology, governance structures, and trust relationships but are not interoperable
- Need to ensure that the right individuals have access to the authorized resources they need regardless of where they reside in the enterprise
- Security and privacy of information are major impediments to information exchange and system interoperability
- Today justice users must subscribe to multiple registration processes and manage multiple security mechanisms and passwords in order to get access to the resources they need
  - This is expensive, frustrating for users, and not scalable

Trust Domains

Trust domains describe the boundaries of a security infrastructure operating under a consistent set of policies, governance, and technology mechanisms.

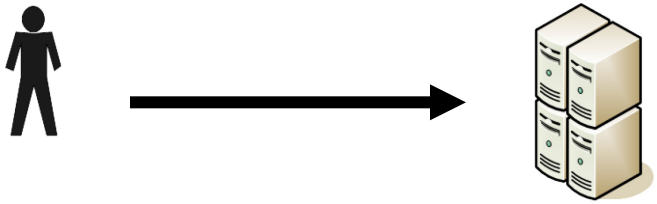
Problem: Authentication and Authorization are typically recognized only within a given trust domain, unless.....

What is required to achieve interoperability across Trust Domains?



One user accessing one application

User Application

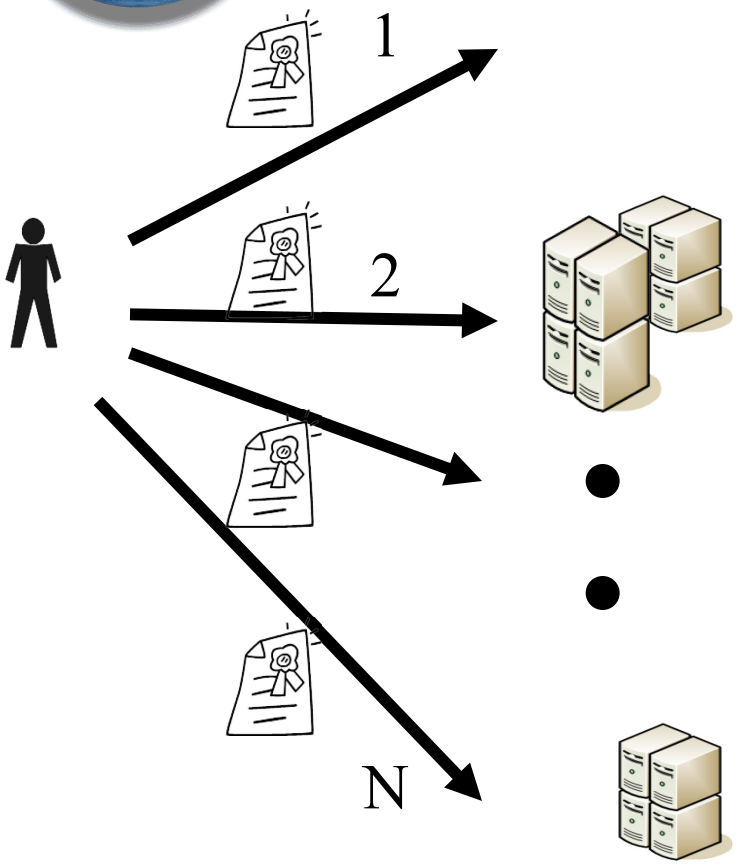


Steps in provisioning access:

- Vetting (who are you?)
- Permissioning (what can you access?)
- Credentialing (how do I know it's you? – passwords, smart cards, etc.)

Access requires authentication of credentials

One user accessing many applications



Steps in provisioning access:

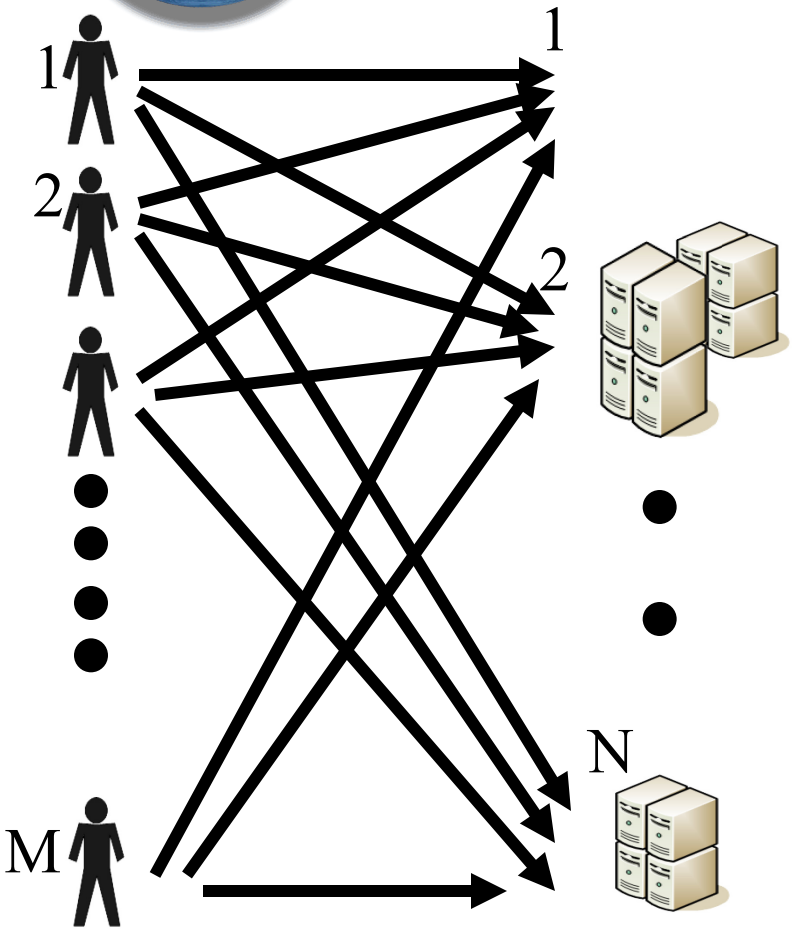
- Vetting
- Permissioning
- Credentialing

× N

RESULT:

- Each application must perform all steps above
- User must keep track of N sets of credentials

Many users accessing many applications



Steps in provisioning access:

- Vetting
- Permissioning
- Credentialing

Expensive!!

× M × N

RESULTS:

- Multifactor credentials & vetting become too expensive
- Vetting & credentialing not done well.
- Vetting too far from user to be kept up to date effectively
- High barrier to access

Federation

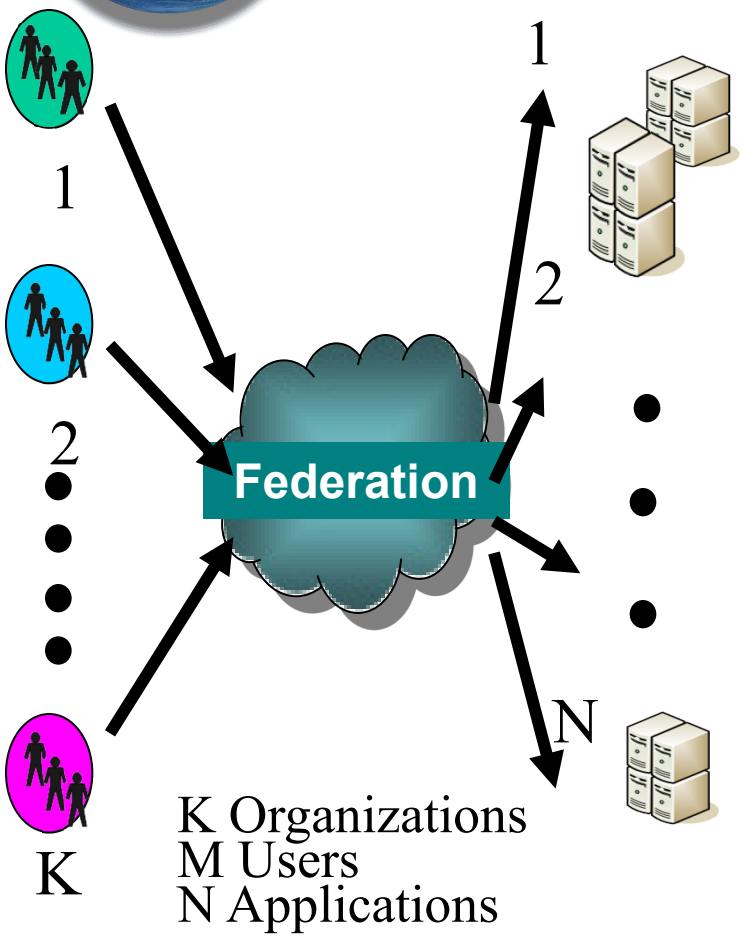
Identity Provider

NIEM Inside

Mutual Trust

Service Provider

Value Proposition

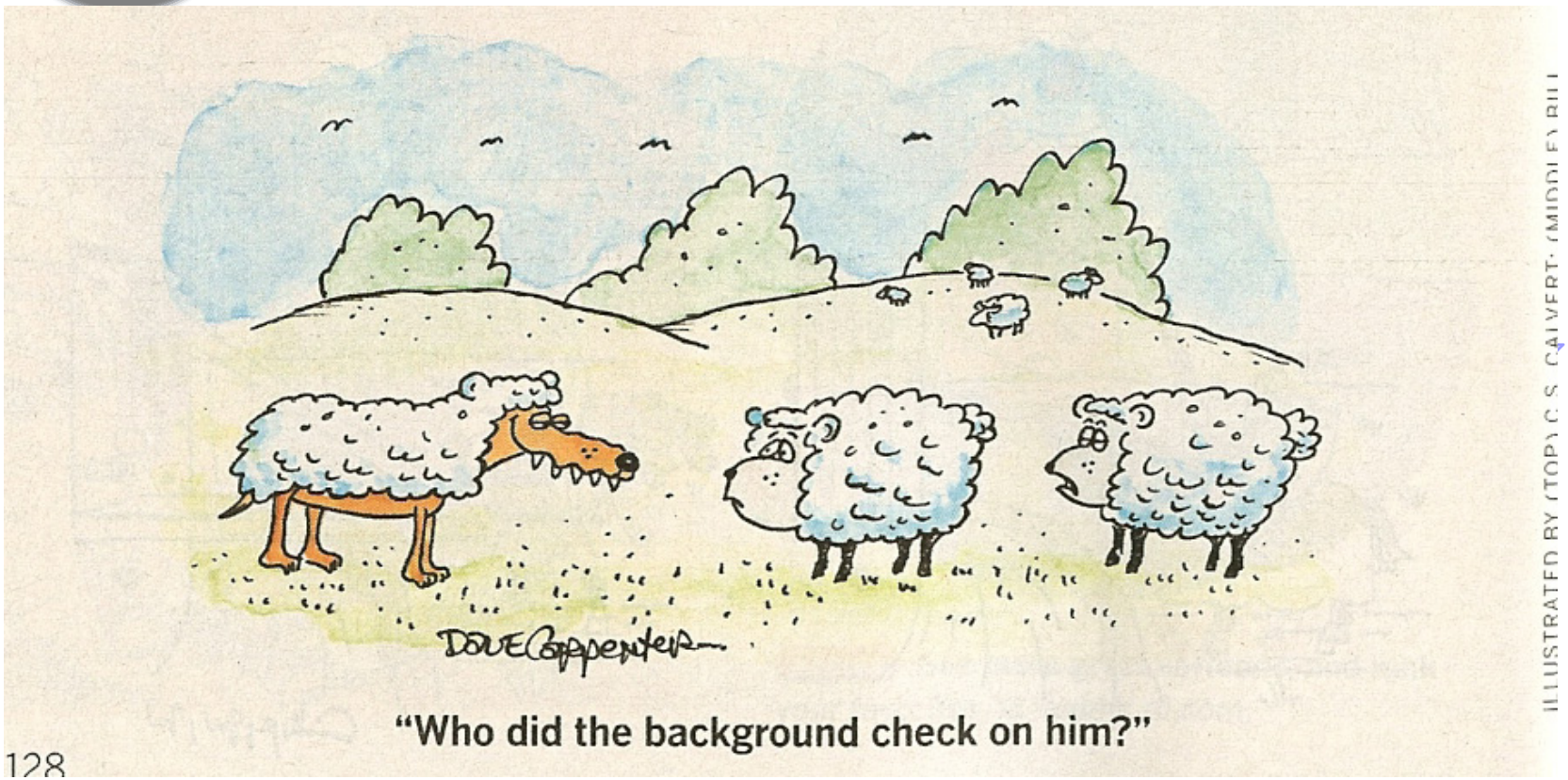


Provisioning identity and user attributes (vetting and credentialing) with the organization (×M)

Applications make access and authorization decisions based on trusted federation credentials and user attributes

RESULTS

- Huge savings in vetting and credentialing M<<M×N
- Vetting is better – closer to the user since own organization does vetting
- Credentialing is better – can afford multifactor
- Each users only needs one credential (Single sign-on)
- Lower barriers to access – more access

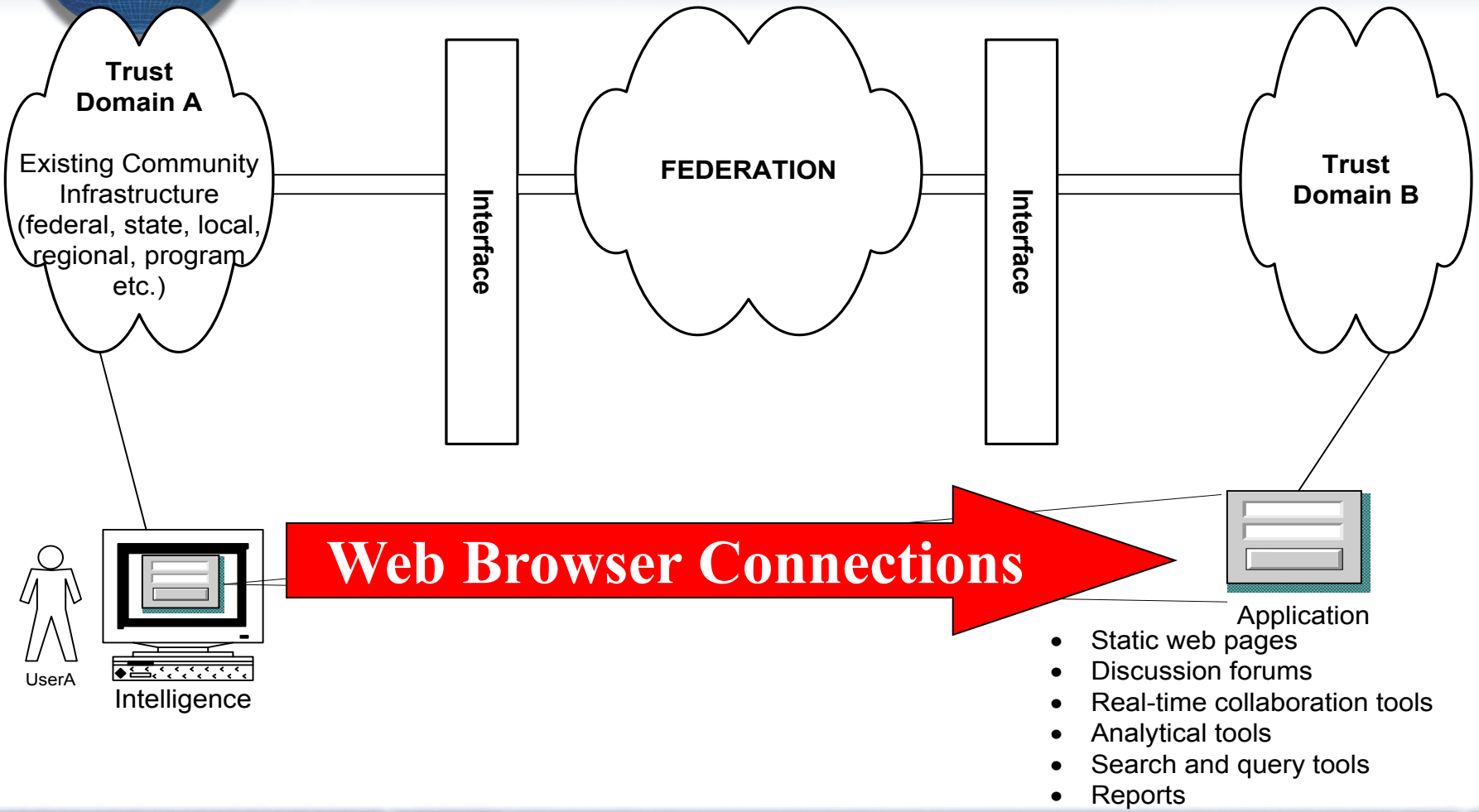


"Who did the background check on him?"

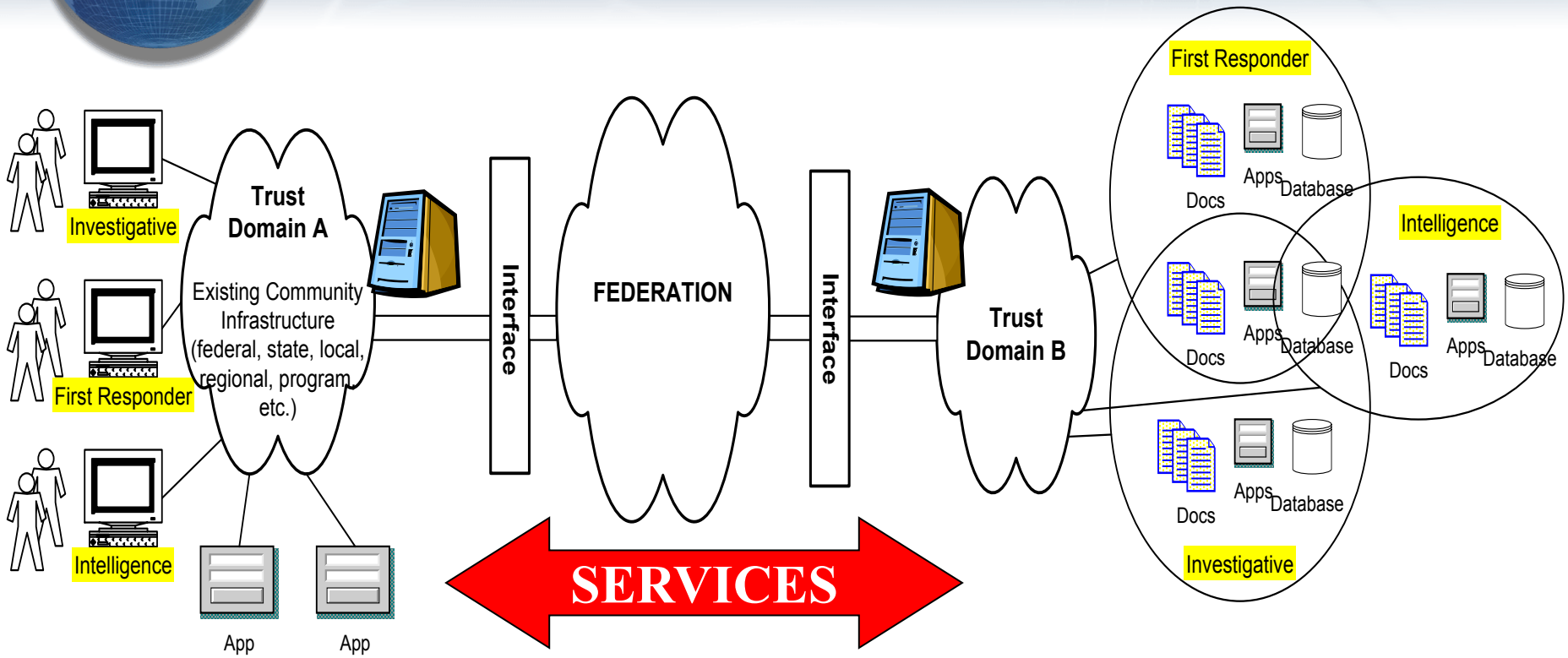
128

Basic Concepts of GFIPM

User-to-Application Use Case



System-to-System SOA Use Case

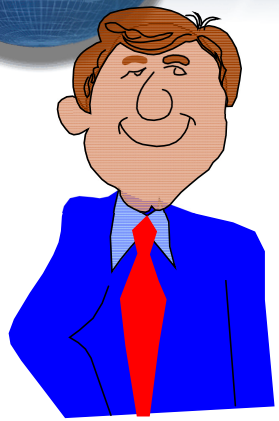


Users gain access to resources and services connected to the Federation through their local enterprise systems and authentication methods. User vetting and maintenace is retained by local enterprise.

Global Justice Information Sharing Initiative

GI adata For ertions

Identity & Electronic Identity



Bob

Identity *– "A* ***unique name*** *corresponding to the* ***real-world*** *person or entity. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique." -* ***NIST***

Electronic Identity

Bob.dsk- Bob's electronic identity stored on a soft token

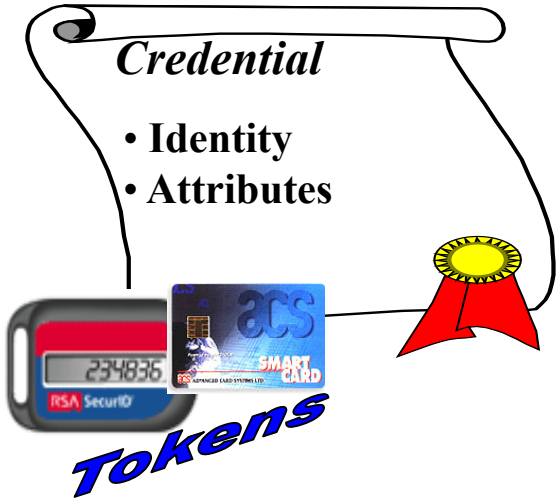
OR

Bob.tkn - Bob's electronic identity stored on a hard token

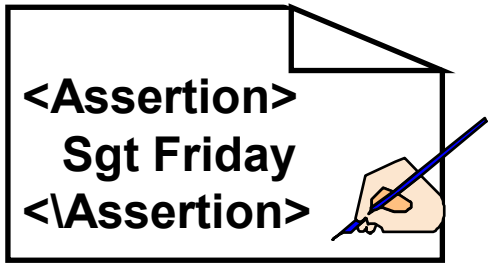
Credentials, Tokens, & Assertions

- **Credential** - An object that authoritatively binds an identity (and optionally additional attributes) to a token possessed and controlled by a person
- **Token** - Something that the user possesses and controls (typically a key or password) used to authenticate the their identity.

Tightly Coupled by Authentication Protocol



- **Assertion** – "A ***trusted statement*** from an Identity Provider to a Service Provider that contains identity information about a subscriber. Assertions may also contain other verified attributes."



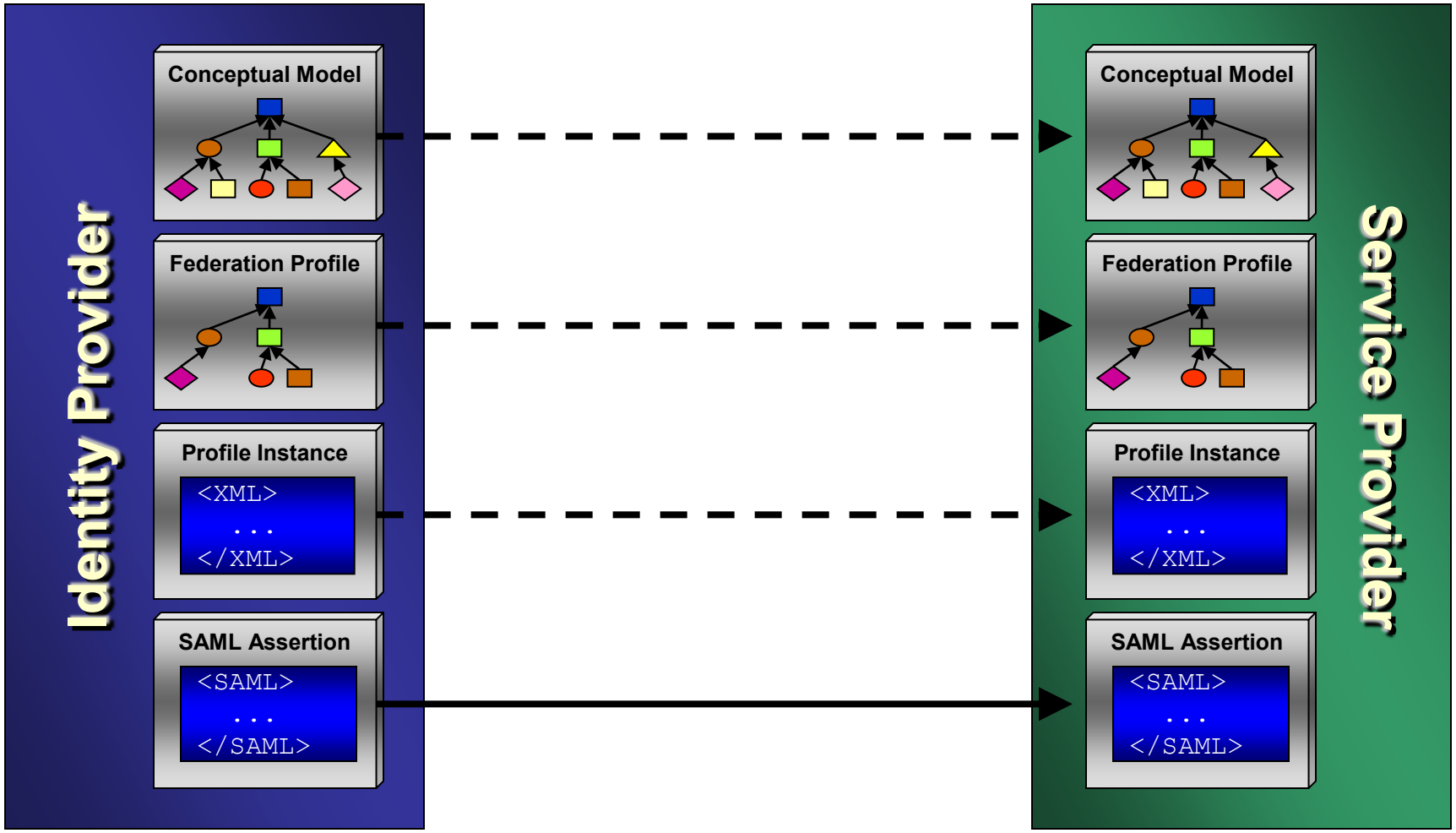
GFIPM Metadata

- Provides a ***common data model*** across federation systems
  - Common ***semantics*** and ***structure*** for metadata associated with federated users and federated entities
- Supports
  - Identification and Authentication
  - Resource Authorization / Privilege Mgmt
  - Auditing / Accountability
  - Personalization
  - Future framework for Privacy Policy Enforcement

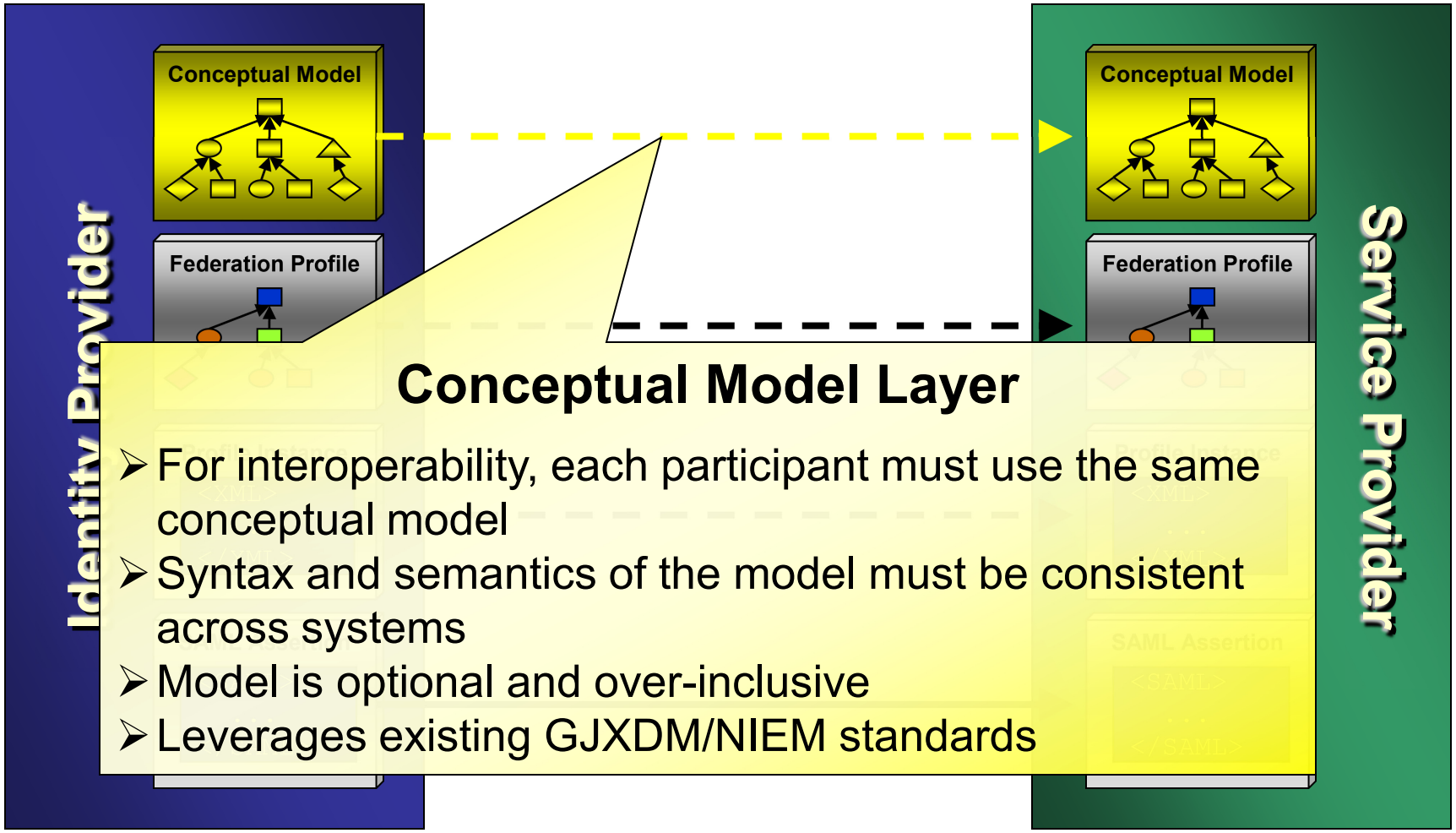
GFIPM Assertion Design Objectives

- Leverage existing GJXDM and NIEM data modeling concepts, principles, architecture, and content (semantics and structure).
- Leverage existing federated identity standards. Specifically, the Security Assertion Markup Language (SAML). Support for other standards and versions in the future is anticipated.
- Leverage other relevant metadata initiatives
  - DHS user attributes for authority based access control
  - Global Technical Privacy Working Group
- Allow for many use cases of FIPM
  - User-to-Application
  - System-to-System (SOA use case)
- Separation of the identification and ***modeling*** of GFIPM Metadata from the ***encoding*** and transport of that metadata between federation participants in a SAML Assertion.

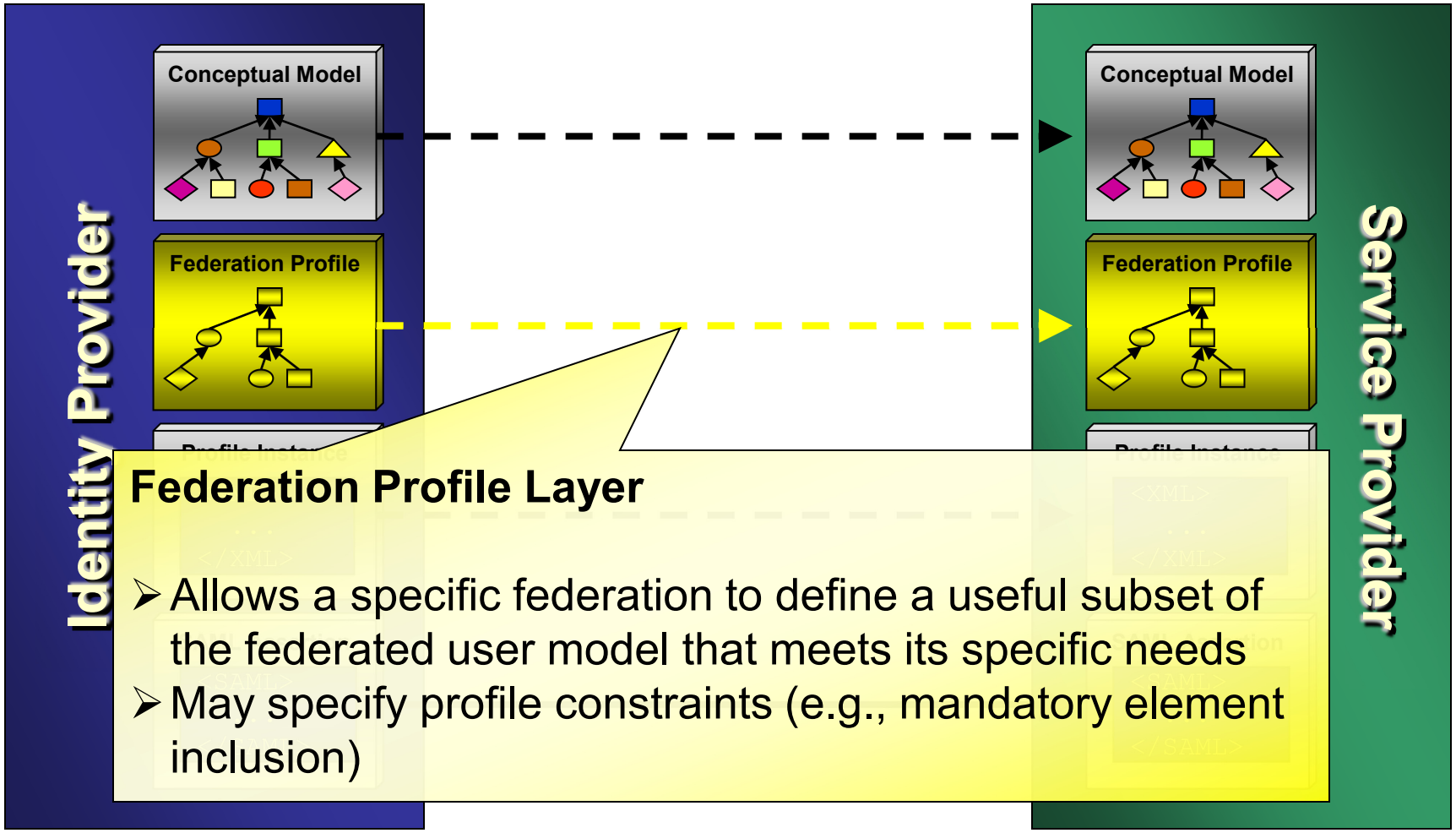
GFIPM Metadata & Assertion Framework



GFIPM Metadata and Assertion Framework



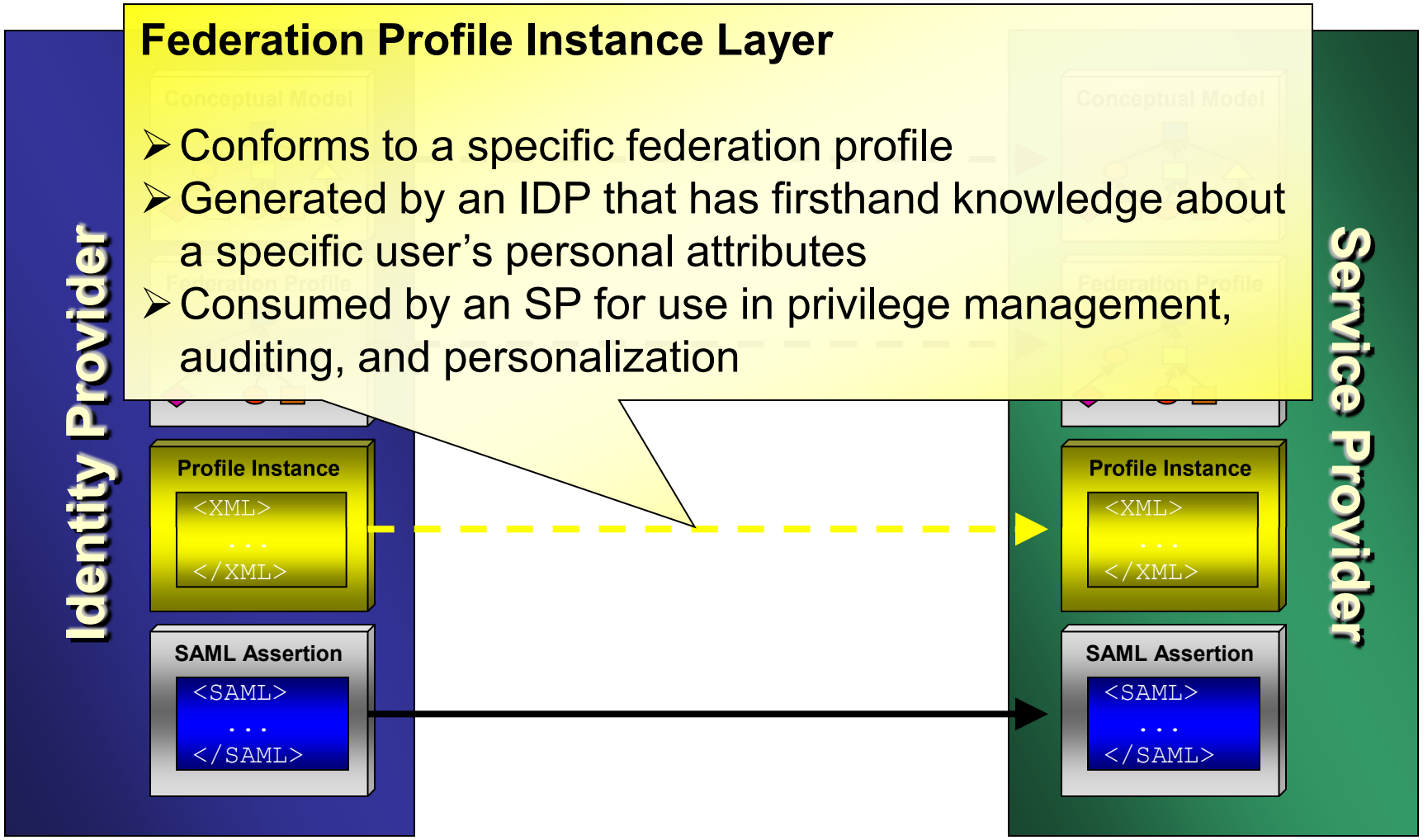
Global FIPM User Assertion Framework



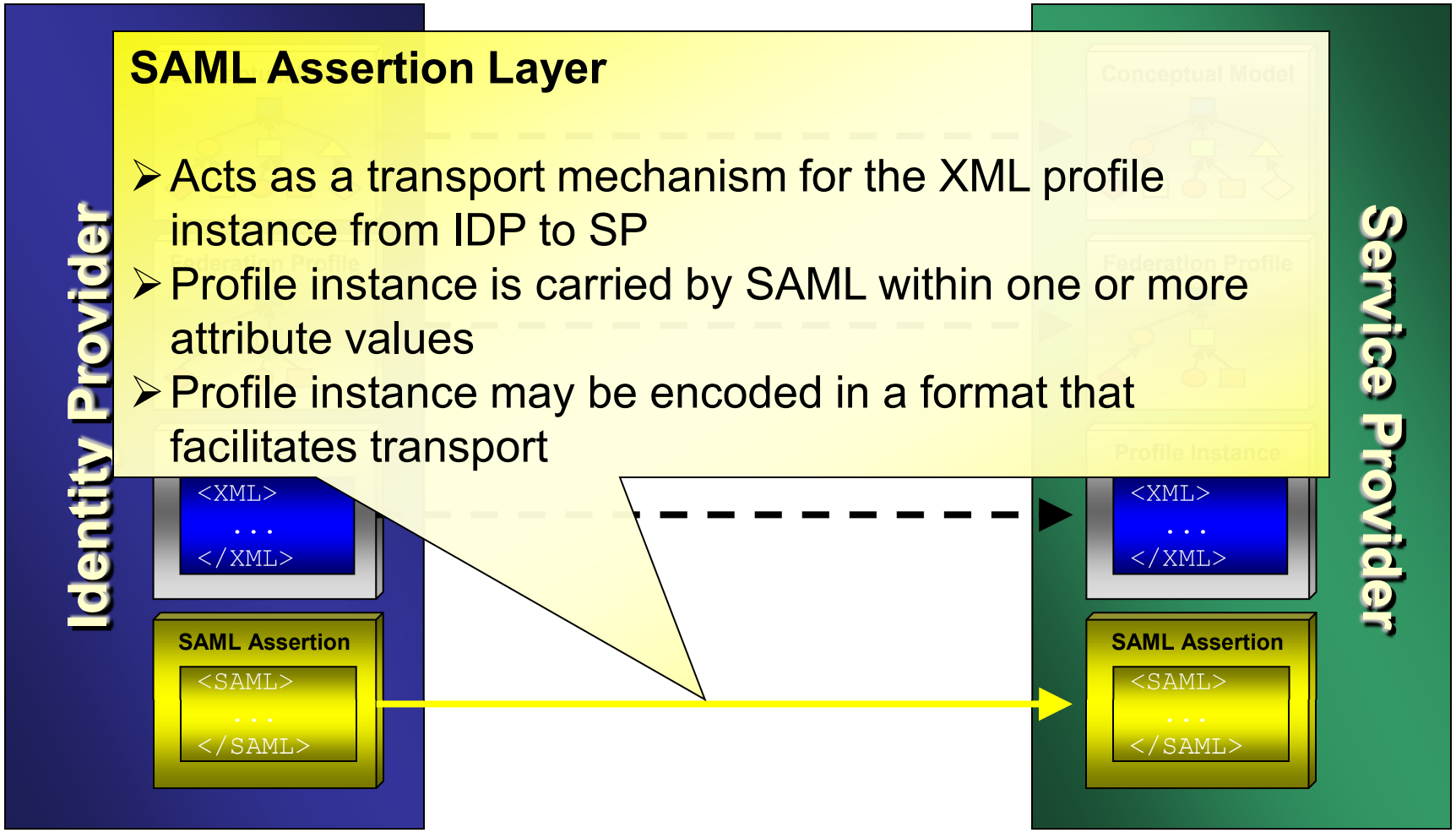
Federation Profile Layer

- Allows a specific federation to define a useful subset of the federated user model that meets its specific needs
- May specify profile constraints (e.g., mandatory element inclusion)

Global FIPM User Assertion Framework



Global FIPM User Assertion Framework

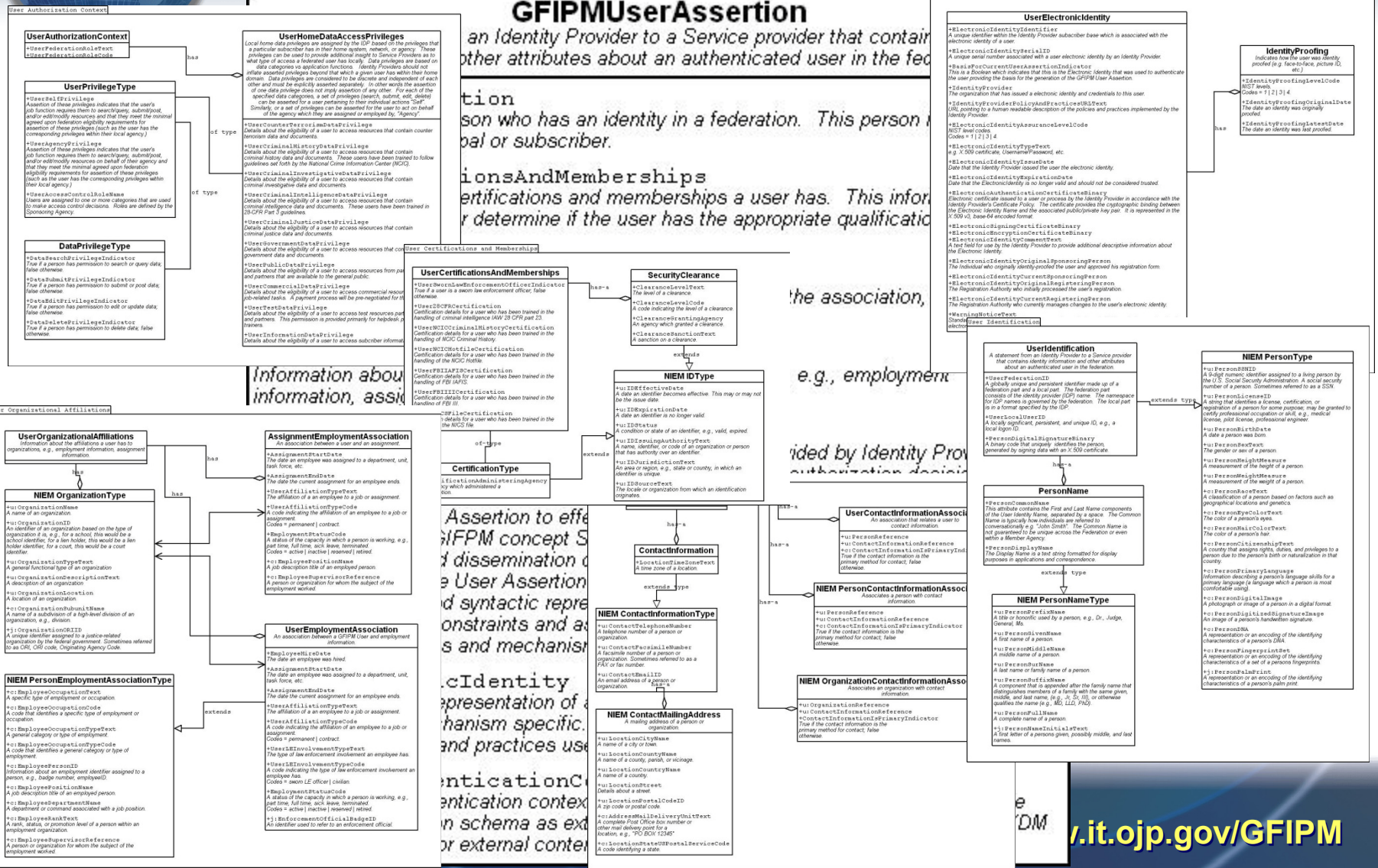


Contents of User Assertion

- **User Identification**
  - *Info about a person who has an identity in the federation*
- **User Certifications and Memberships**
  - *Can help an SP make access control decisions*
- **User Contact Information**
  - *Contact info for the user, his/her supervisor, employer, etc.*
- **User Organizational Affiliations**
  - *Info about the user's employment status, assignments, etc.*
- **User Authorization Context**
  - *Supplemental info to help an SP make access control decisions*
- **User Electronic Identity**
  - *Info about the user's electronic identity (type, issue date, etc.)*
- **User Authentication Context**
  - *Incorporates SAML 2.0 authentication context*

Global Justice Information Sharing Initiative

User Assertion



http://it.ojp.gov/GFIPM

SAML Assertions are XML!

```
<Assertion
   xmlns="urn:oasis:names:tc:SAML:1.0:assertion"
   AssertionID="_19ef0cd871a089eb5f8d262fa8813885"
   IssueInstant="2006-06-26T19:16:33.369Z"
   Issuer="global:gfipm:linuxrefidp"
   MajorVersion="1" MinorVersion="1">
 <Conditions NotBefore="2006-06-26T19:16:33.369Z" NotOnOrAfter="2006-06-26T19:46:33.369Z">
  <AudienceRestrictionCondition>
   <Audience>global:gfipm:linuxrefsp</Audience>
  </AudienceRestrictionCondition>
 </Conditions>
 <AttributeStatement>
  <Subject>
   <NameIdentifier
     Format="urn:mace:shibboleth:1.0:nameIdentifier"
     NameQualifier="global:gfipm:linuxrefidp">
     _51d57480b10a61e4fb987ba6b98ea9c6
   </NameIdentifier>
  </Subject>
  <Attribute AttributeName="FederationPersonName"
             AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
    <AttributeValue>George Burdell</AttributeValue>
  </Attribute>
  <Attribute AttributeName="UserID"
             AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
    <AttributeValue>gburdell</AttributeValue>
  </Attribute>
 </AttributeStatement>
</Assertion>
```

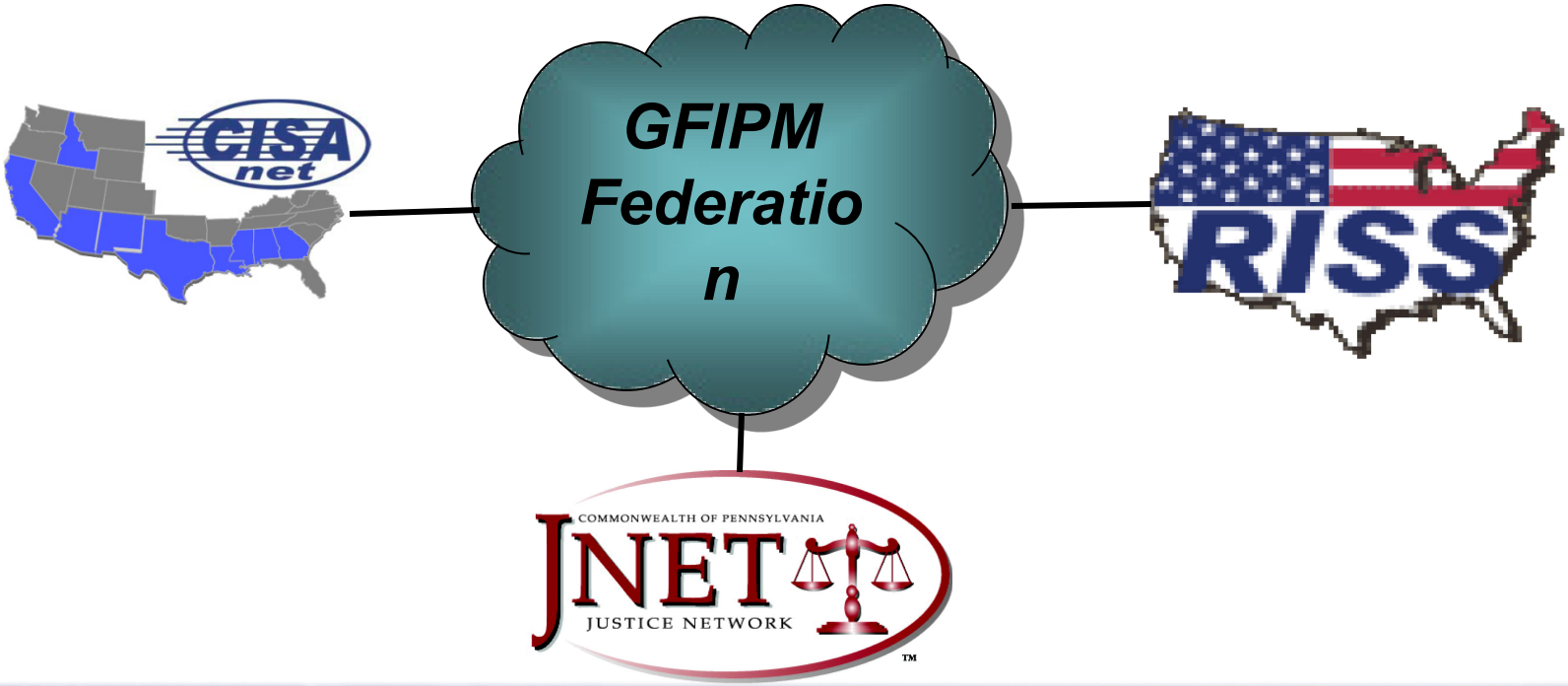
Design Process and Timeline

- ✓ Identified & collected metadata based on survey results from GSWG member systems.
- ✓ Grouped/harmonized survey results and mapped them to NIEM to create a "strawman" data model: GFIPM Metadata 0.1.
- ✓ Vetted strawman via GFIPM Tiger Team and DOJ/DHS Demo Project participants to create GFIPM Metadata 0.2
- ✓ Incorporated feedback and corrections between v0.2,v0.3 and (current) v0.4. Currently used in demonstration pilot.

- Update for NIEM 2.0 content and structures – Fall 07
- Publish draft for broader vetting – Fall 07
- Currently evaluating alternative methods for encoding GFIPM Metadata in SAML to yield a standard GFIPM assertion representation and support by COTS products

Global Justice Information Sharing Initiative

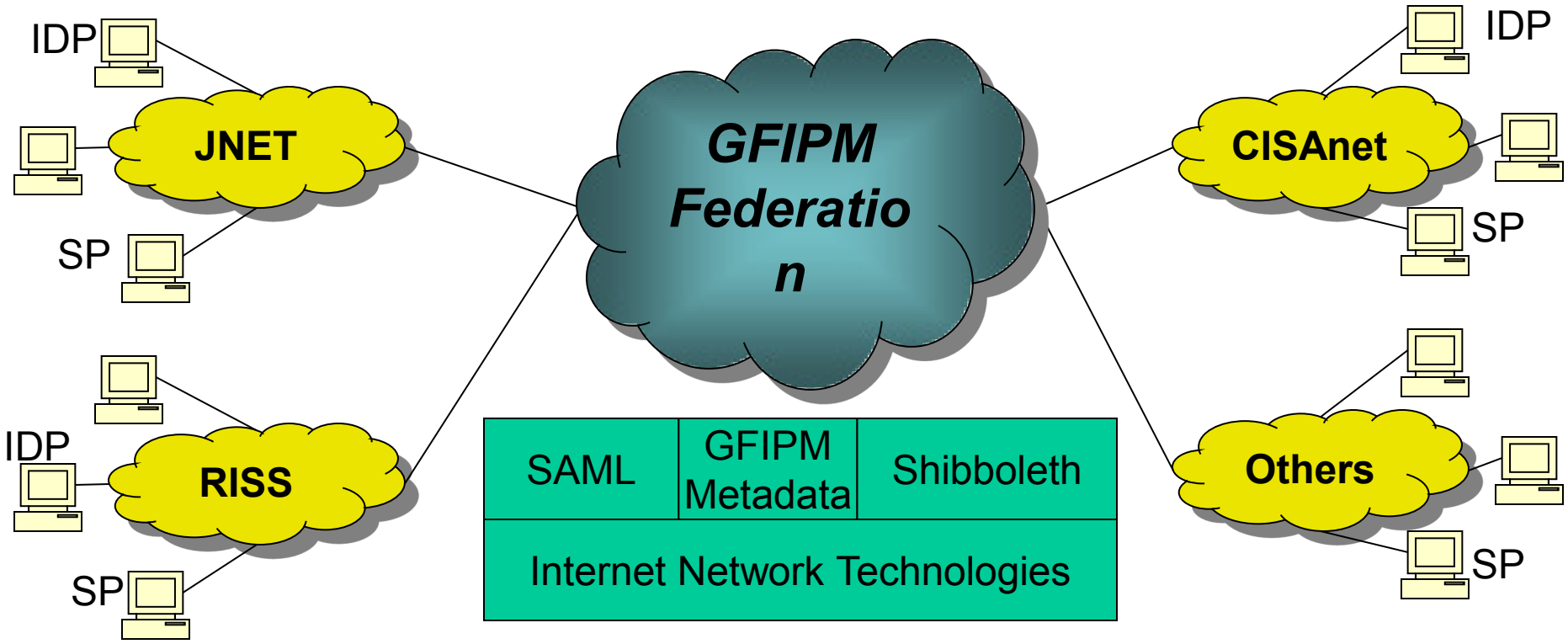
GFIPM Security Interoperability Demonstration Project



Project Initiation and Funding

- GFIPM project was initiated by the Global Security Working Group in 2005 in response to the National Criminal Intelligence Sharing Plan (NCISP)
- Funded jointly by Bureau of Justice Assistance (BJA), National Inst. of Justice (NIJ), and Dept. of Homeland Security (DHS) Office of Chief Info Officer (OCIO)
- Initial project phase included three existing networks within the justice community
  - Criminal Info Sharing Alliance Network (CISAnet)
  - Pennsylvania Justice Network (JNET)
  - Regional Information Sharing Systems Network (RISSNET)
- Project mgmt, engineering, and technical assistance provided by Georgia Tech Research Institute (GTRI)

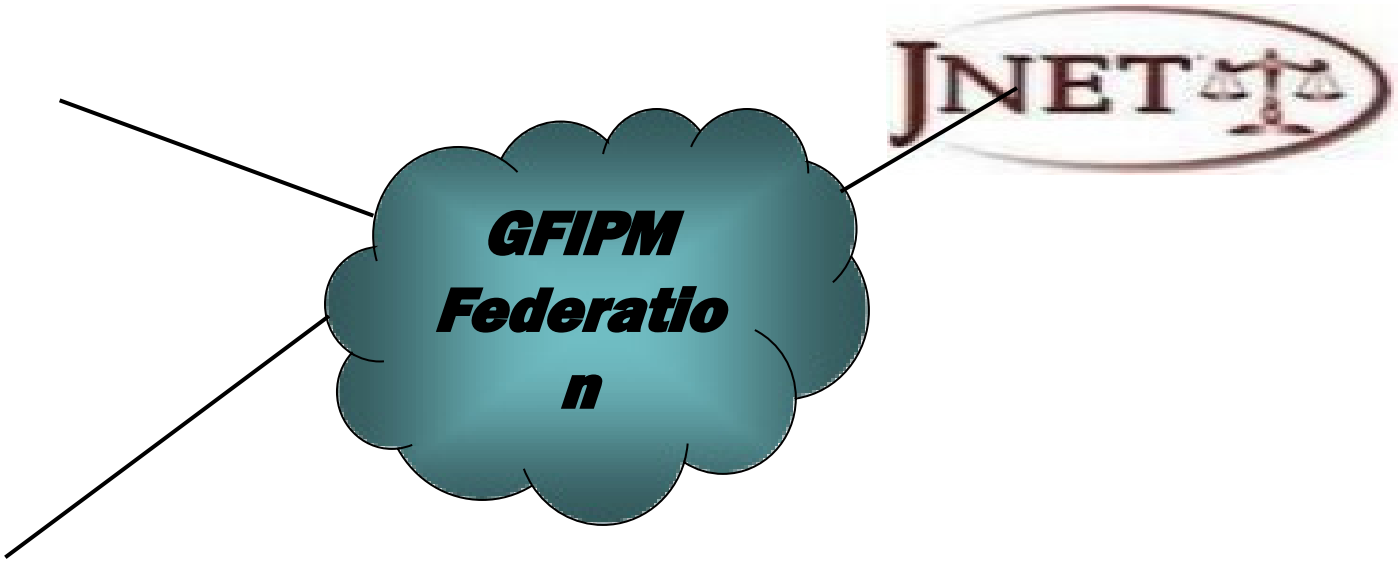
Project Approach



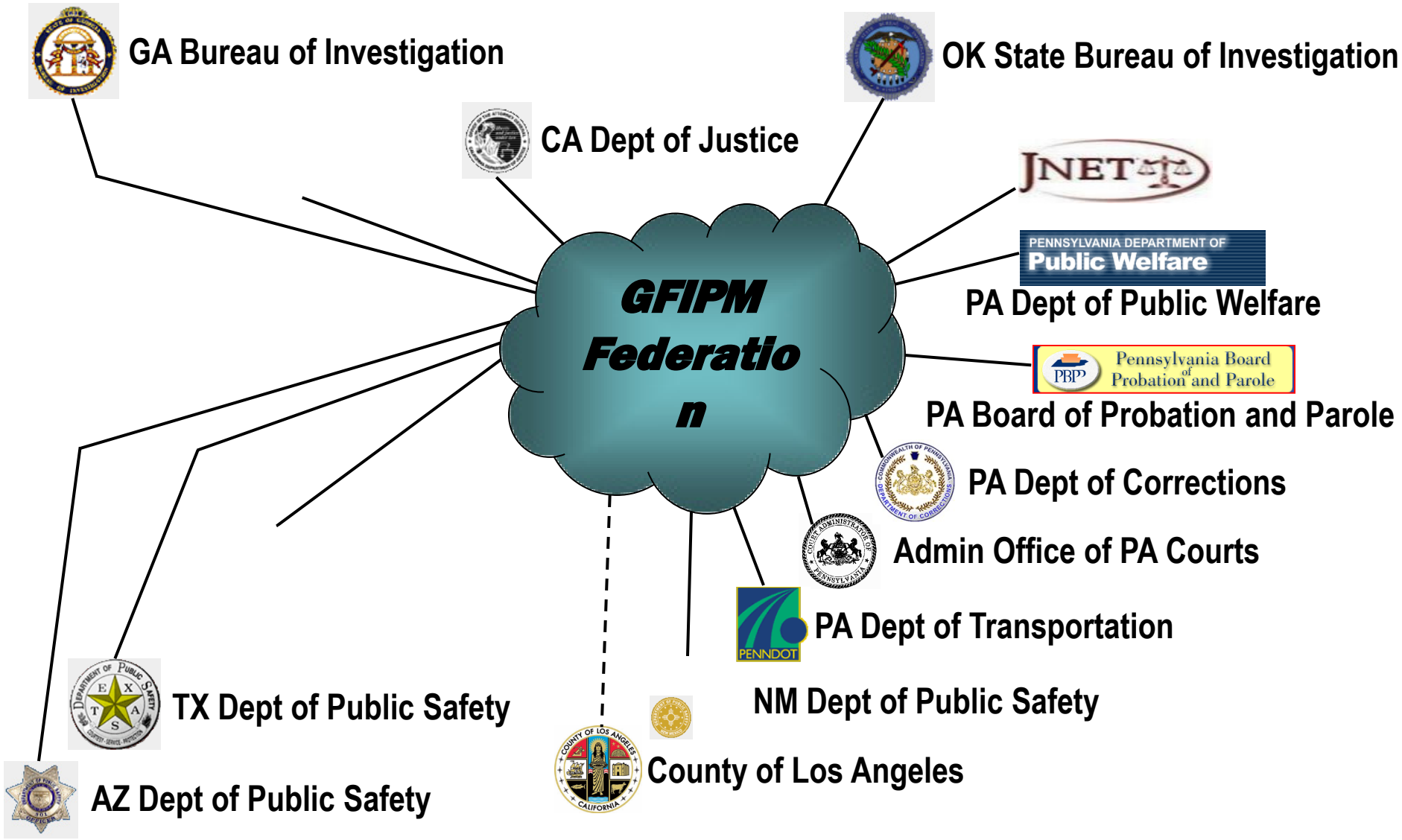
- Leverage existing participant subscriber base and infrastructure
- Initially focused on Law Enforcement
- Agreed upon set of attributes (semantics, syntax, NIEM-based)
- User-to-application use case (browser to Web app)

- Authorization decisions are made by SPs based on metadata passed in SAML assertions
- Use of Internet, Federation Standards, and open source
- Use of standard SSL/TLS encryption and server side authentication

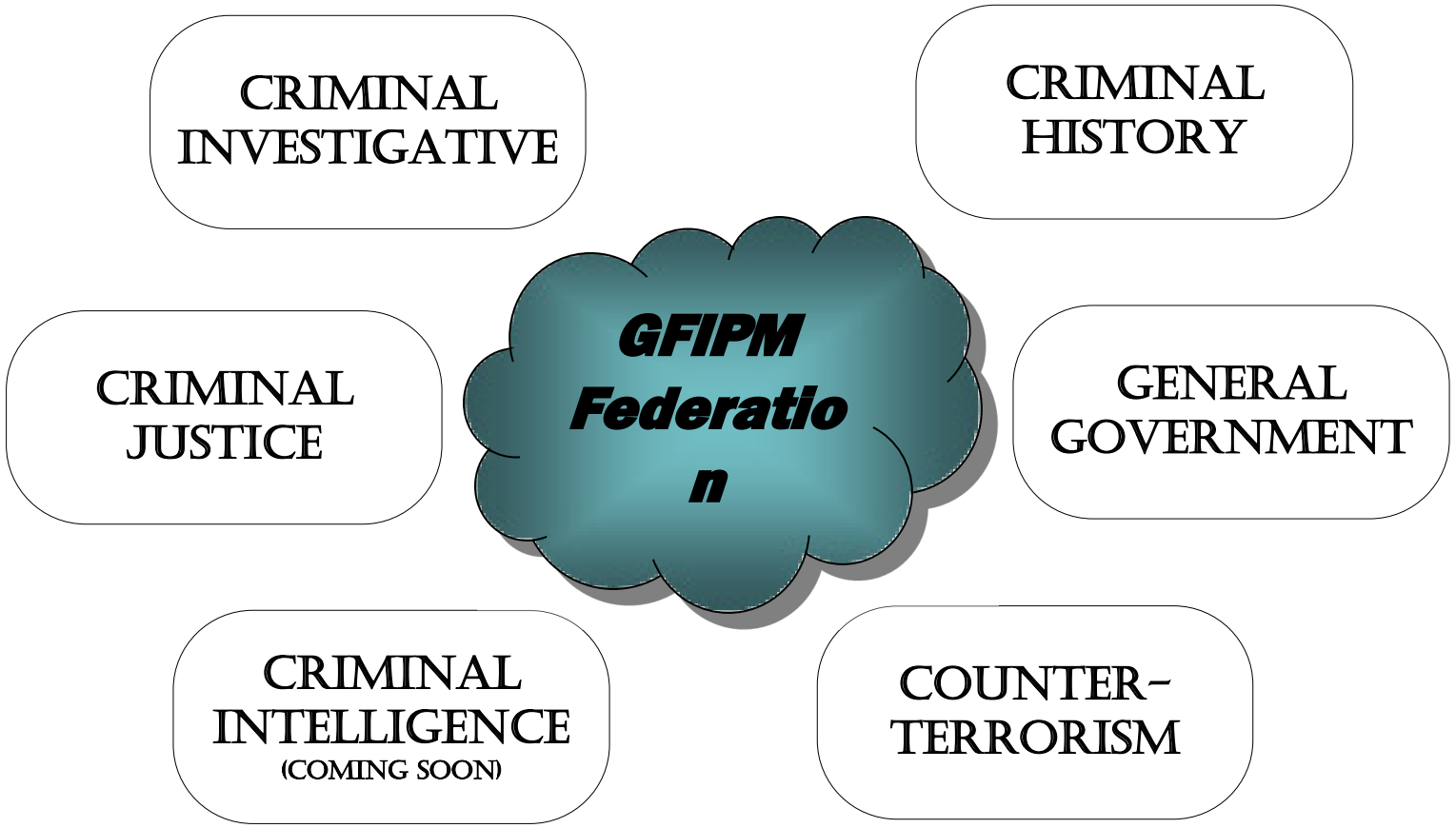
GFIPM Participating Agencies



GFIPM Participating Agencies



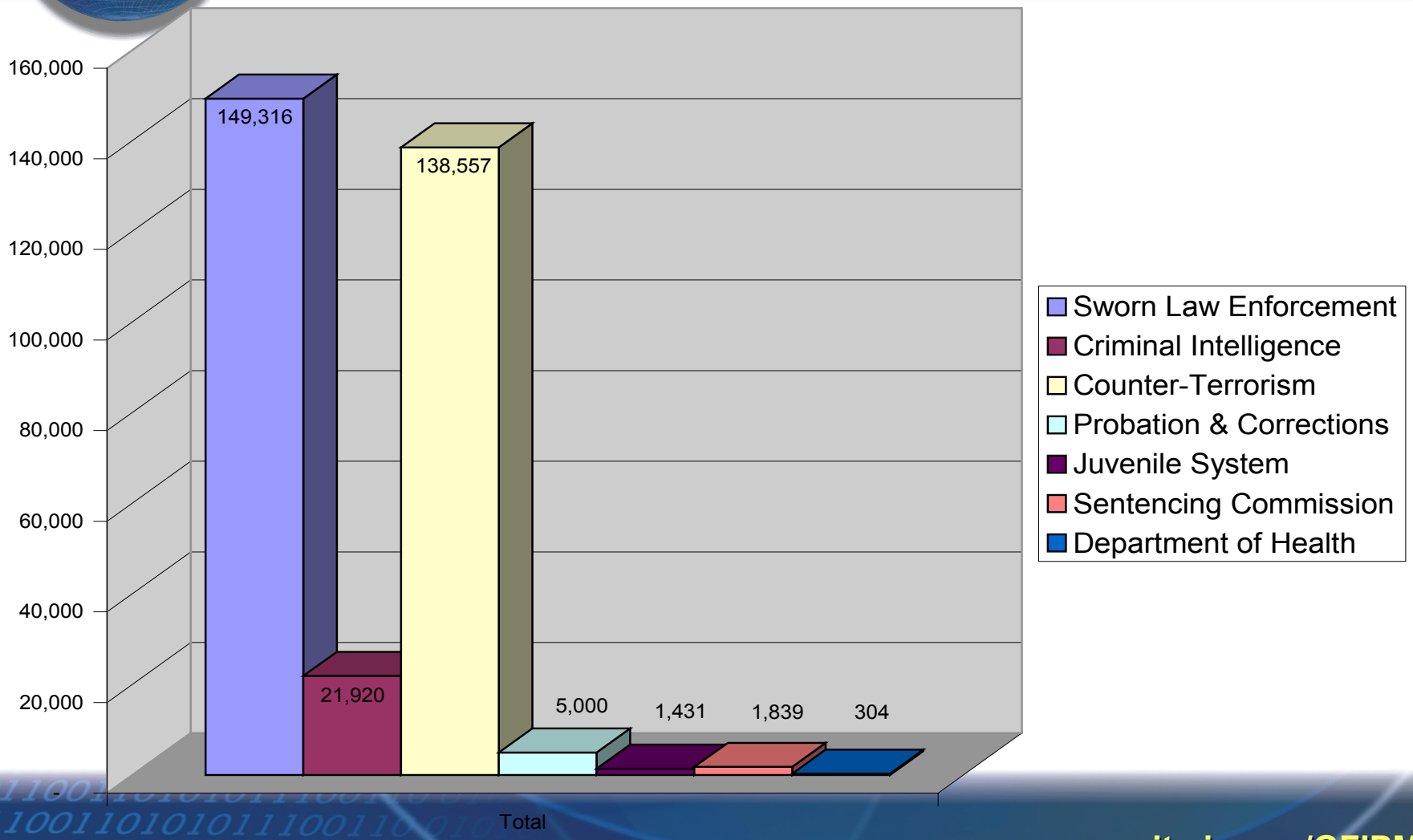
GFIPM Resources



GFIPM Resources

- Texas Criminal Law Enforcement Reporting and Information System
- RISS Counter-Terrorism Data Repository
- Arizona Criminal Investigative Database
- Arizona Counter-Terrorism Information Center
- New Mexico Incident-Based Reporting System
- Pennsylvania Criminal Trial Case Information
- Pennsylvania Driver's License Photos (Coming Soon)
- Georgia Bureau of Investigation Sex Offender Registry
- New Mexico Missing Persons & Unidentified Bodies
- Criminal Law Enforcement Reporting and Information System
- White Pages of Pennsylvania Justice Staff (Coming Soon)
- Pennsylvania Arrest Warrants Outstanding for Failure to Pay Child Support
- Pennsylvania Department of Corrections Intake/Exit Photos
- Pennsylvania Probation "Fail to Report" Photos and Cases
- California Joint Regional Information Exchange System
- Oklahoma State Bureau of Investigation Officer Safety Bulletin
- New Mexico Law Information Information Network with Corrections
- Los Angeles County Consolidated Criminal History (Integration Testing)
- Texas Criminal Law Enforcement Online
- New Mexico Sex Offender Registration
- Georgia Bureau of Investigation JIMnet
- HSIN Counter-Terrorism Data Repository
- Arizona Sex Offender Information Center
- Pennsylvania State Prisoner Locator
- New Mexico Complete Arrest Information
- CISAnet Federated Query Tool
- Pennsylvania Amber Alert
- Arizona Amber Alert

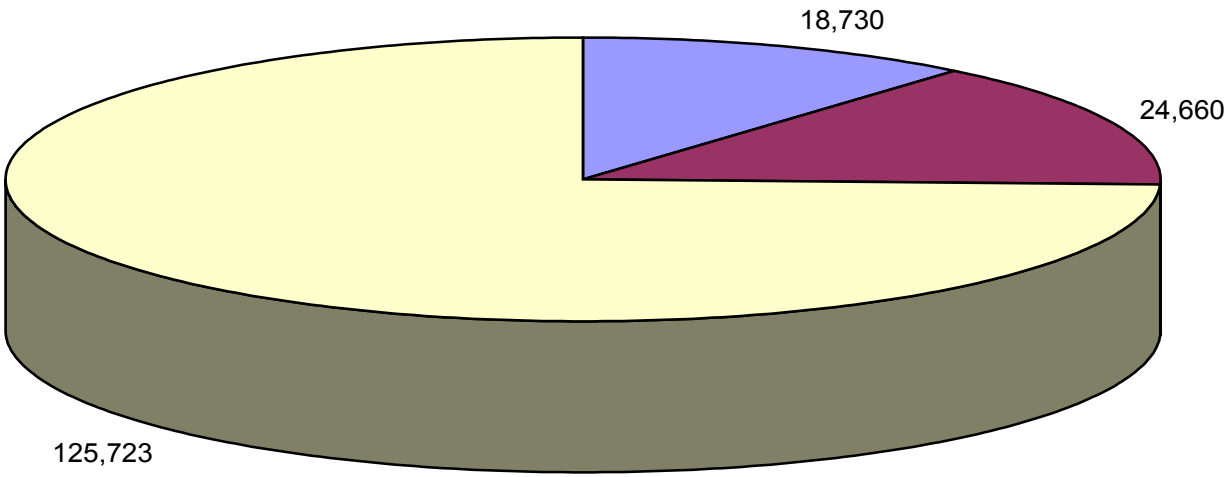
GFIPM User Demographics



Global Justice Information Sharing Initiative

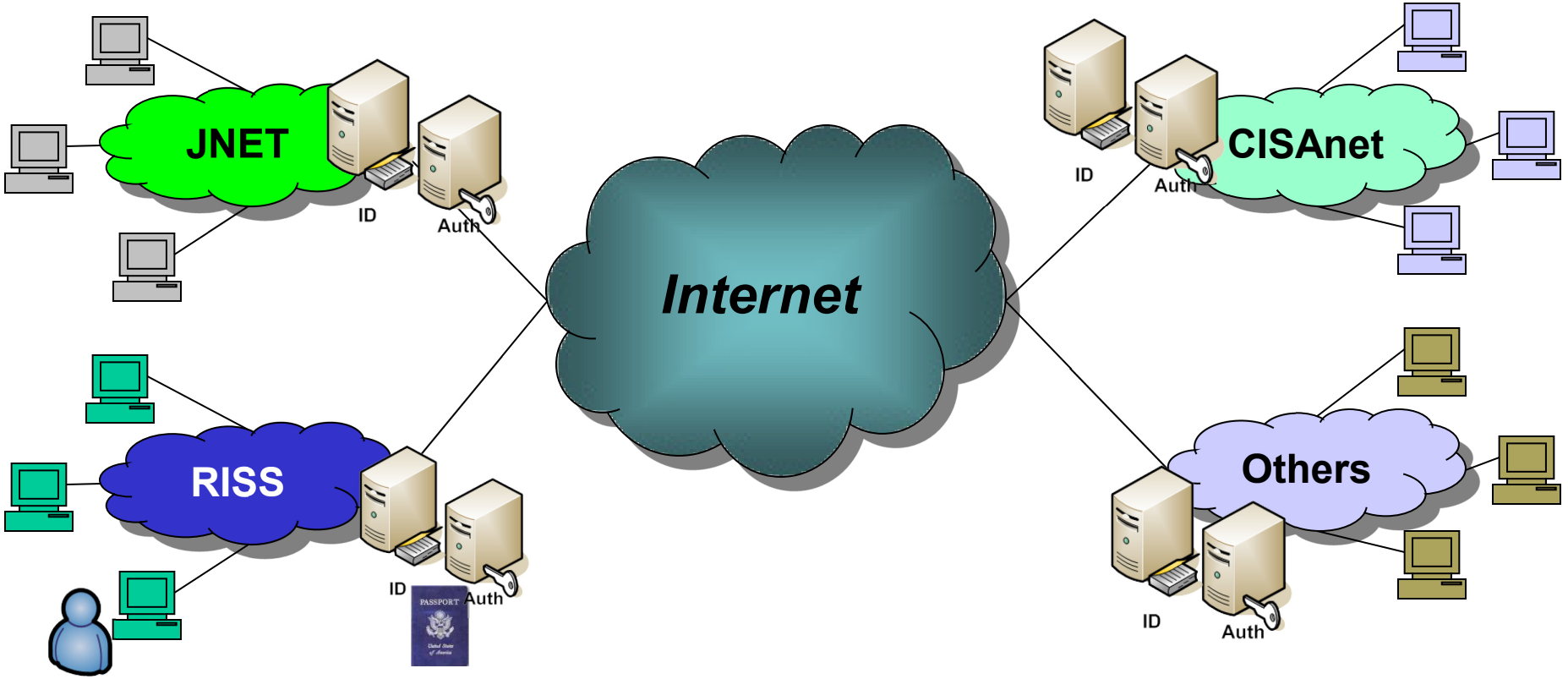
Total

GFIPM User Demographics

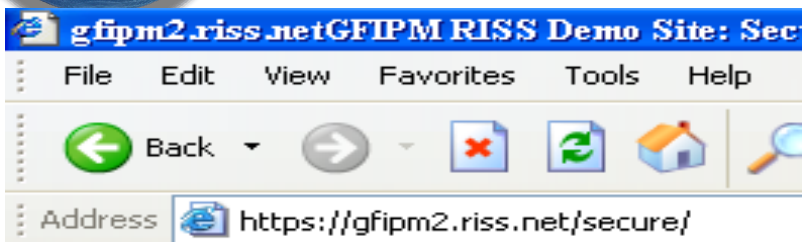


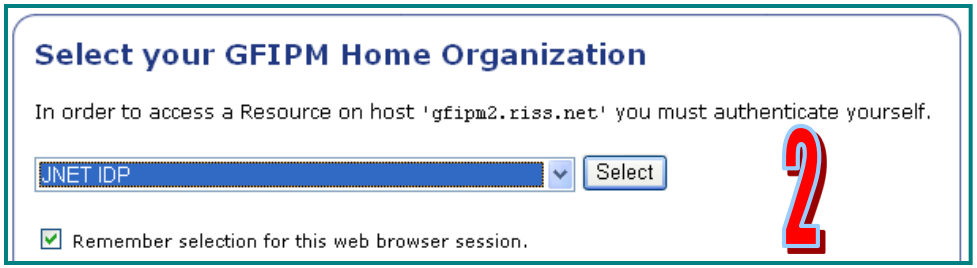
Total Potential Users ~170,000

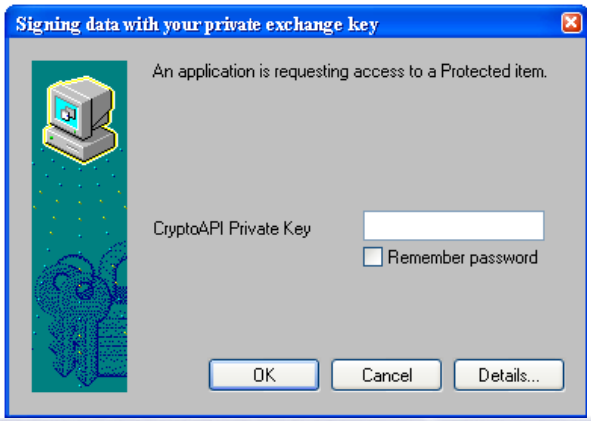
How does it work?

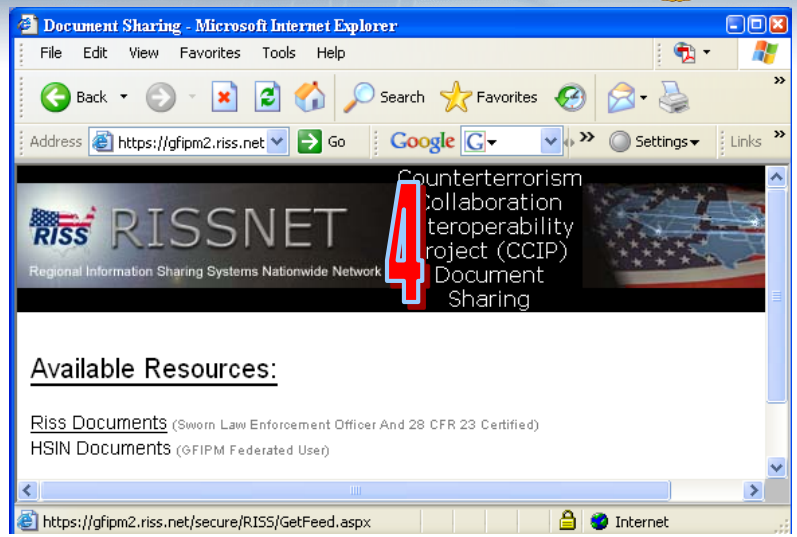


How It Works
User Perspective



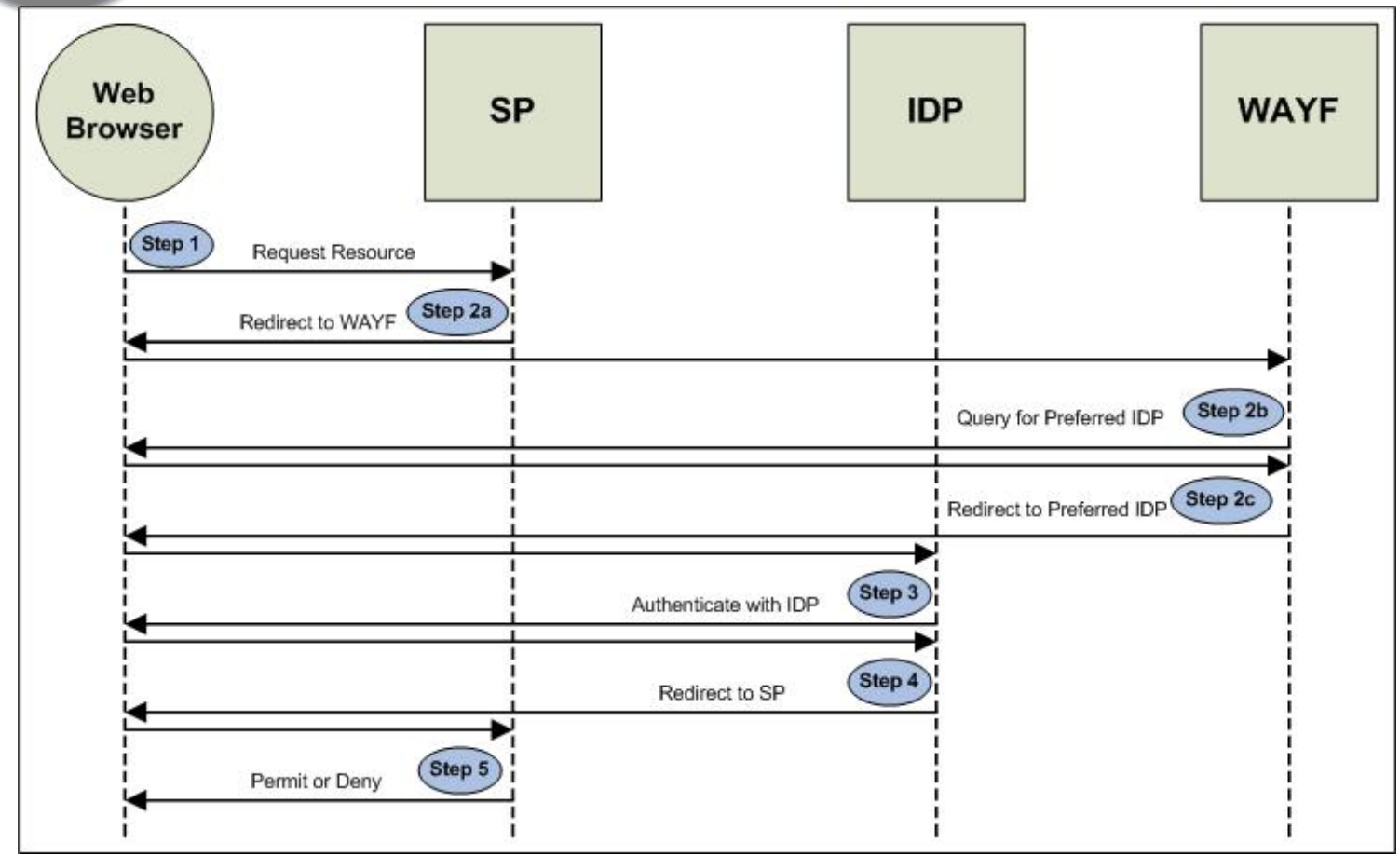




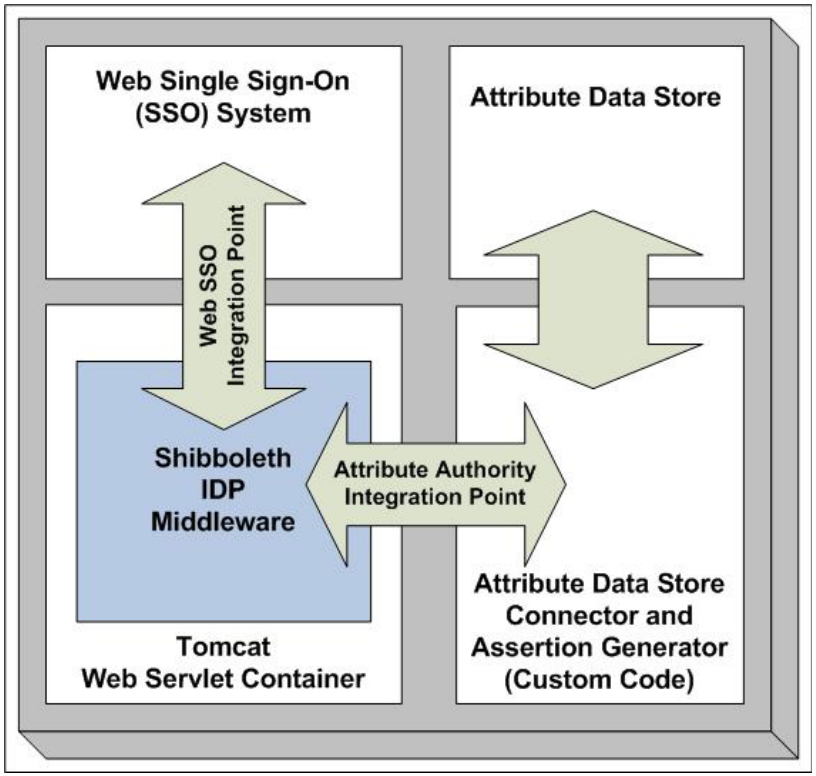


1. JNET user tries to link to RISS.
2. RISS asks user to identify their home agency.
3. JNET (the home agency) prompts the user for authentication credentials.
4. RISS accepts the authentication and privileges presented by JNET.

How It Works
Technical Perspective



Identity Provider Integration



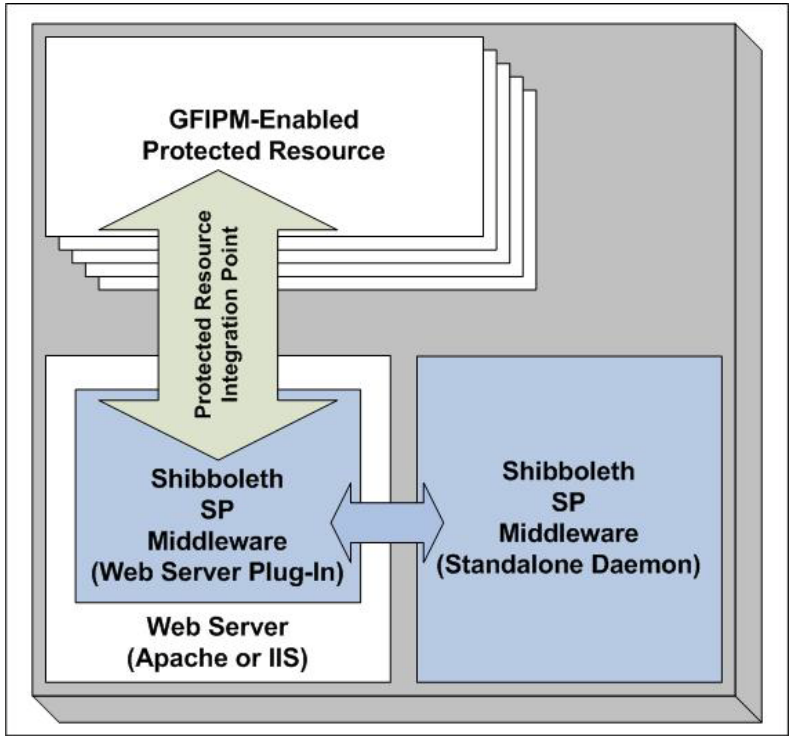
Single Sign-On (SSO) Integration Point

Must configure IDP to authenticate local users with the desired authentication system (e.g. certificate, username/password, vendor specific, etc.)

Attribute Repository Integration Point

Must configure IDP to collect necessary GFIPM Metadata from local repository (e.g. LDAP) and prepare it for encoding as GFIPM Assertion

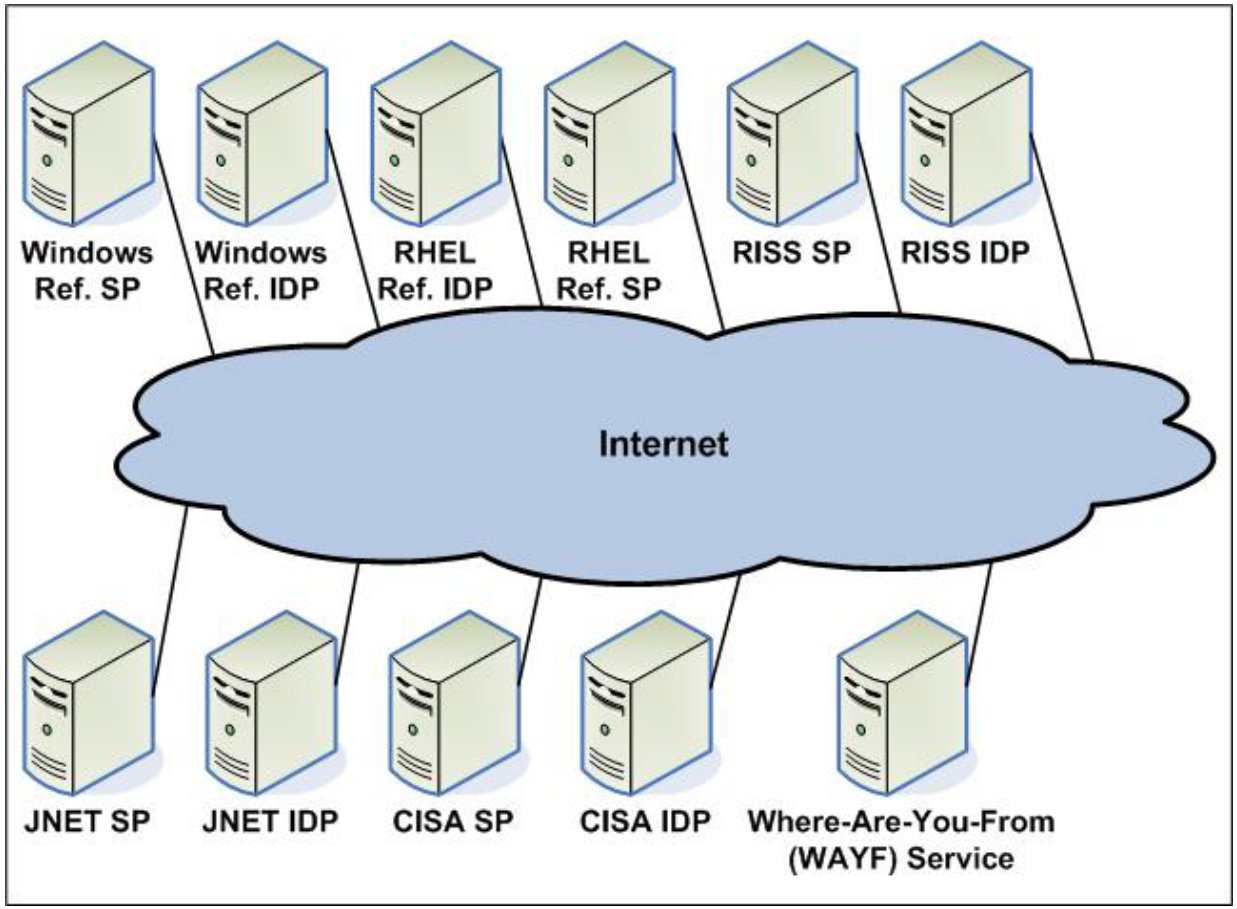
Service Provider Integration



Protected Resource Integration Point

Must configure Service Provider to consume GFIPM Assertion, extract GFIPM Metadata, and mediate access to protected resources with it

Reference Federation



Global Justice Information Sharing Initiative

Lessons Learned Highlights

GFIPM Federation

GFIPM Concept
Lessons Learned Highlights

Global Justice Information Sharing Initiative

Concept has proven to be viable

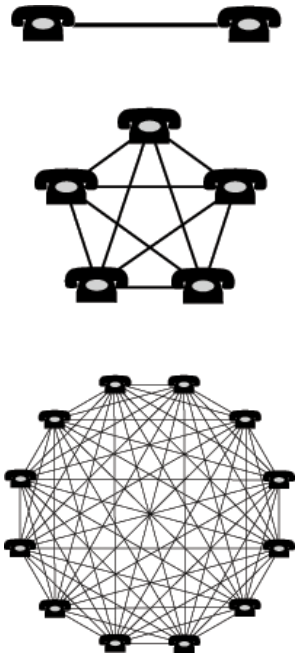
- Leverage existing vetted users and mechanism
- Authorization can be granted based on attributes
- Sufficiently security
- Performance
- Single sign-on across multiple agency applications

Business Case

Lessons Learned Highlights

Business Case (when and why to join?)

- Metcalfe's law applies, early adopters
- Demographics for users and resource access requirements required
- SP decision, IDP decision
- A myriad of potential business arrangements exist (direct, brokers, inter-federation, etc)



GFIPM Metadata
Lessons Learned Highlights

- Agreement on metadata for identification and authorization was possible
- Required user attributes were either already being collected and stored by agencies or could be derived based on others or policy
- Attribute based access control vs. role based access control
- A standard for encoding GFIPM metadata in SAML assertions was necessary
- Based on limited scope and number of participants

GFIPM Enablement

Lessons Learned Highlights

Federation Enablement of Legacy Resources

- Identity Providers tended to be simpler to integrate then Service Providers
- Federation facing services need to be built
- Many enablement options each with advantages and disadvantages
- Resource integration patterns and techniques emerged
- The need for a reference federation capability to support testing between IDPs and SPs

GFIPM Enablement
Lessons Learned Highlights

Resource Integration Profiles

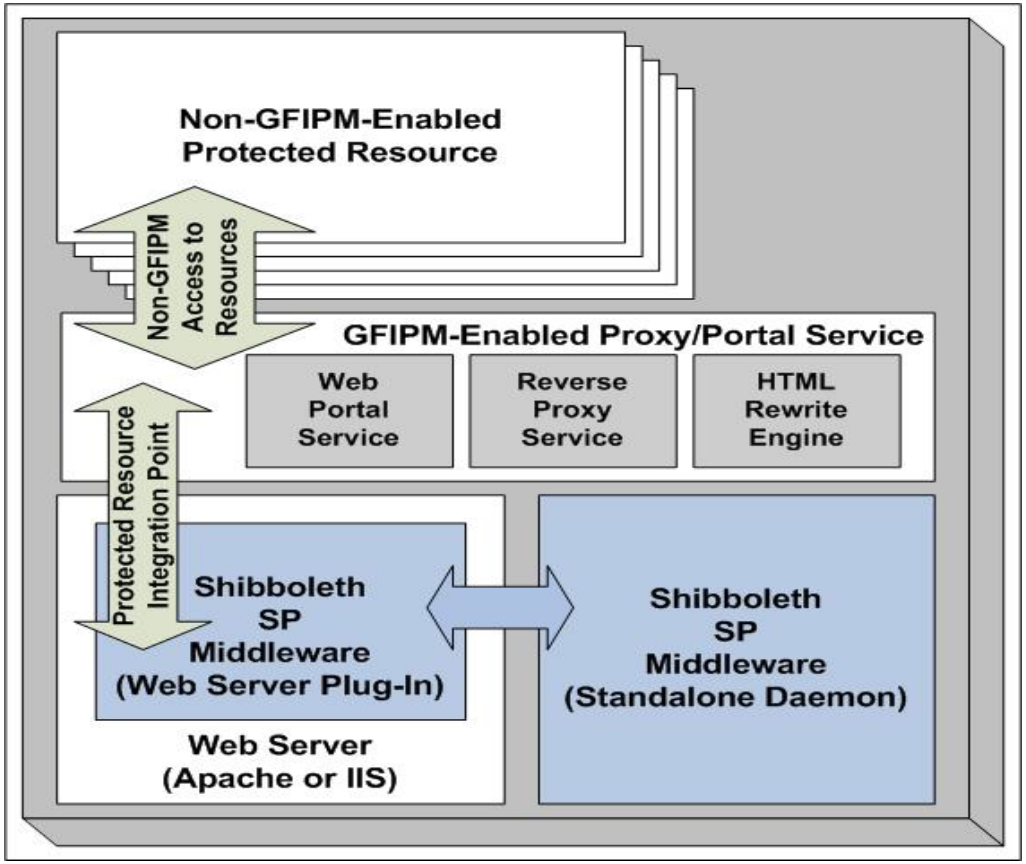
- Read-Only Content without Individual User Accounts
- Individual User Accounts and Dynamic Provisioning
- Individual User Accounts and Pre-Provisioning

Resource Integration Techniques

- GFIPM-Aware Reverse Proxy with No Secondary Authorization
- GFIPM-Aware Reverse Proxy with Secondary Authorization
- Native GFIPM Enablement

GFIPM Enablement

Lessons Learned Highlights



- A GFIPM-aware proxy can significantly reduce the time and cost for integrating certain classes of legacy applications.

- A generic proxy capability was developed and is being considered as a reusable part of the GFIPM toolkit.

GFIPM Enablement

Lessons Learned Highlights

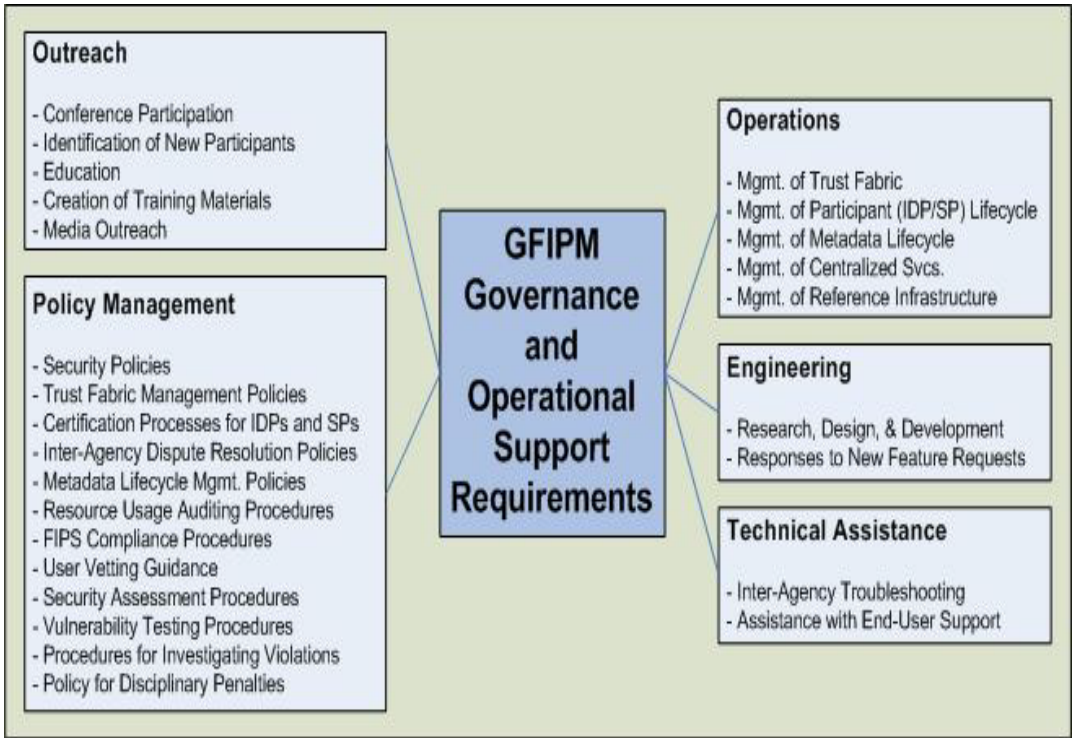
Resource Name	Integration Profile	Integration Technique
Arizona Counter-Terrorism Information Center (ACTIC)	1	1
California Joint Regional Information Exchange System (JRIES)	3	2
Pennsylvania Department of Corrections Intake/Exit Photos	3	2
Pennsylvania Arrest Warrants Outstanding for Parolees who failed to report (Absconders)	3	2
Pennsylvania State Prisoner Locator	3	2
CISAnet Federated Query Tool	2	3
Pennsylvania Arrest Warrants Outstanding for Failure to Pay Child Support	3	2
HSIN Counter-Terrorism Briefs, Reports, and Documents	1	3
⋮	⋮	⋮
⋮	⋮	⋮

Usability and Support
Lessons Learned Highlights

Usability and Support

- Search and discovery of resources – "GFIPM Google" or federation directory services
- User access requirements – consistency across federation
- Training
- Support and help desk functions

Governance and Operations
Lessons Learned Highlights



- A formal governance structure with participation from the federation membership will need to be established to develop and lifecycle manage federation policies and procedures
- On going operational support to carry out day-to-day processes and procedures related the federation will be required

Participant Comments

Demonstration provides real operational value today!

"The FIPM concept of trusting a federation member agency's own registration system to provide the most accurate and current identity and home privilege information on a user is unquestionably the most reasonable approach to take if data sharing among agencies is to be done at a national level." - JNET

"RISS considers the Federated Identity Management model as the most appropriate approach to sharing information with its autonomous partners." - RISS

Global Recommendations

- Recognize GFIPM as the recommended approach for development of interoperable security functions for authentication and privilege management for information exchange among cross-domain justice information sharing systems.
- Urge the members of the justice community to consider GFIPM as a potential building block to a layered security solution when authenticating uses among cross-domain organizations.

Next Steps

- Global GFIPM Delivery Team
- Establish Formal Governance
- Update, Validate, and Vet GFIPM Standards
- Migrate to SAML 2.0 and support COTS products
- Provide tools/assistance/documentation to reduce time and cost of joining the federation
- Extend GFIPM concepts and standards to support Global's Justice Reference Architecture
- Expand the Pilot Federation (participants, users, resources)
- Establish and test inter-federation data exchanges

Resources

- Monitor www.it.ojp.gov/GFIPM for more information
- Coming Soon…
  - Draft GFIPM Metadata Specification
  - Project Report
  - Presentations

Global Justice Information Sharing Initiative

Questions ?